明細書

防御装置、防御方法および防御プログラム並びにネットワーク攻撃防御システム

技術分野

[0001] この発明は、ネットワーク上のサーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御装置、防御方法および防御プログラム並びにネットワーク攻撃防御システムに関する。

背景技術

[0002] 従来より、DoS(DenialofService)攻撃またはDDoS(DistributedDenialofService)攻撃を受けるネットワーク上のサーバを防御する防御装置と、サーバに送信されるパケットを中継する複数のルータとをネットワーク上に備えたネットワーク攻撃防御システムが知られている。例えば、特許文献1(米国特許出願公開第2002／0083175号明細書)に開示されたネットワーク攻撃防御システムでは、サーバに対する攻撃を検出した場合に、防御装置は、パケットを自己に経由させるための経路情報を所定のルータに通知することによって、自己を経由するパケットのフィルタリングを行い、フィルタリングを行ったパケットをサーバに転送する。

[0003] これについて、図13を用いて具体的に説明する。図13は、従来技術に係るネットワーク攻撃防御システムを説明するための図である。同図に示すように、例えば、通信端末94(攻撃者)がサーバ92(被害者)に対して攻撃を行っている場合、攻撃検知装置95は、ルータ83を経由してパケットを受信するサーバ92が攻撃を受けていることを検知すると、攻撃を検知したことを防御装置90に通知する(図13の(1)および(2)参照)。そして、この通知を受けた防御装置90は、パケットを自己に経由させるための経路情報を所定のルータ93に通知する(同図の(3)参照)。その一方、ルータ93は、受信した経路情報に基づいてルーティング表を更新し、更新したルーティング表に従ってパケットを中継する(同図の(4)参照)。すなわち、ルータ93は、サーバ92向けの攻撃パケットを防御装置90に転送するようになる。その結果、防御装置90は、ルータ93から転送された攻撃パケットのフィルタリングを行い、フィルタリングを行っ

たパケットをルータ83を介してサーバ92に転送する。

[0004] 特許文献1:米国特許出願公開第2002／0083175号明細書(第10頁－第12頁)

発明の開示

発明が解決しようとする課題

[0005] しかしながら、上記した従来の技術では、例えば、図13に示した例のように、ルータ83を経由してパケットを受信するサーバ92に対する攻撃を検出した場合にだけ、防御装置90が経路情報をルータ93に通知することが予め決まっているため、仮にサーバ92が攻撃者になったような場合には攻撃パケットを防御することができないという問題がある。すなわち、従来技術に係るネットワーク攻撃防御システムでは、攻撃パケットの流入方向が固定されていなければ攻撃に対応できないという問題がある。

[0006] また、従来技術に係るネットワーク攻撃防御システムでは、防御装置90がフィルタリングを行ったパケットをルータ93に転送するときに、防御装置90とルータ93との間でパケットのループが生じてしまうという問題もある。さらに、これらの問題の他に、上記した従来の技術では、ネットワーク攻撃防御システムが複数の防御装置90を備えるようにした場合において、所定のルータ93に経路情報を通知することが予め決まっているため、攻撃パケットの送信元に一番近い防御装置に攻撃パケットを迂回させて攻撃パケットの通過を制御することができず、攻撃パケット送信元に一番近い防御装置だけに攻撃パケットを経由させて攻撃パケットを迂回することもできないといった問題がある。

[0007] そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、攻撃パケットの流入方向に影響されることなく攻撃パケットを防御することなどが可能な防御装置、防御方法および防御プログラム防御プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

課題を解決するための手段

[0008] 上述した課題を解決し、目的を達成するため、請求項1に係る発明は、ネットワーク上のサーバまたはドメインに対する攻撃情報に基づいて、当該サーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御装置であって、前記攻撃情報に基づいて、自己に隣接する

複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択手段と、前記中継装置選択手段によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知手段と、前記経路情報通知手段によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御手段と、を備えたことを特徴とする。

[0009] また、請求項2に係る発明は、上記の発明において、前記中継装置選択手段は、自己に隣接する複数の中継装置のなかから前記攻撃パケットによる攻撃を受けているサーバまたはドメインに対して次の中継先となる中継装置を除いて、前記経路情報の通知先となる中継装置を選択することを特徴とする。

[0010] また、請求項3に係る発明は、上記の発明において、自己と隣接関係をもつ他の防御装置に対して前記攻撃情報を送信する攻撃情報送信手段をさらに備え、前記中継装置選択手段は、前記他の防御装置から前記攻撃情報を受信した場合にも、当該攻撃情報に基づいて前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択することを特徴とする。

[0011] また、請求項4に係る発明は、上記の発明において、前記経路情報通知手段によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットを監視して、当該中継装置から自己に経由される攻撃パケットの送信が終了したか否かを判定する攻撃終了判定手段をさらに備え、前記経路情報通知手段は、前記攻撃終了判定手段によって前記攻撃パケットの送信が終了したものと判定された場合に、当該攻撃パケットを自己に経由させないための経路情報を前記中継装置に通知することを特徴とする。

[0012] また、請求項5に係る発明は、ネットワーク上のサーバまたはドメインに送信されるパケットを中継する複数の中継装置と、当該サーバまたはドメインに対する攻撃情報に基づいて所定の中継装置に対して経路情報を送信し、当該サーバまたはドメイン宛の攻撃パケットの通過を制御する防御装置とを有するネットワーク攻撃防御システムであって、前記防御装置は、前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先と

なる少なくとも一つの中継装置を選択する中継装置選択手段と、前記中継装置選択手段によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知手段と、前記経路情報通知手段によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御手段と、を備えたことを特徴とする。

[0013] また、請求項6に係る発明は、ネットワーク上のサーバまたはドメインに対する攻撃情報に基づいて、当該サーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御装置による防御方法であって、前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択工程と、前記中継装置選択工程によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知工程と、前記経路情報通知工程によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御工程と、を含んだことを特徴とする。

[0014] また、請求項7に係る発明は、上記の発明において、前記中継装置選択工程は、自己に隣接する複数の中継装置のなかから前記攻撃パケットによる攻撃を受けているサーバまたはドメインに対して次の中継先となる中継装置を除いて、前記経路情報の通知先となる中継装置を選択することを特徴とする。

[0015] また、請求項8に係る発明は、上記の発明において、自己と隣接関係をもつ他の防御装置に対して前記攻撃情報を送信する攻撃情報送信工程をさらに含み、前記中継装置選択工程は、前記他の防御装置から前記攻撃情報を受信した場合にも、当該攻撃情報に基づいて前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択することを特徴とする。

[0016] また、請求項9に係る発明は、上記の発明において、前記経路情報通知工程によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットを監視して、当該中継装置から自己に経由される攻撃パケットの送信が終了したか否かを判定する攻撃終了判定工程をさらに含み、前記経路情報通知工程は、前記攻

撃終了判定工程によって前記攻撃パケットの送信が終了したものと判定された場合に、当該攻撃パケットを自己に経由させないための経路情報を前記中継装置に通知することを特徴とする。

[0017] また、請求項10に係る発明は、ネットワーク上のサーバまたはドメインに対する攻撃情報に基づいて、当該サーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御方法を防御装置としてのコンピュータに実行させる防御プログラムであって、前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択手順と、前記中継装置選択手順によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知手順と、前記経路情報通知手順によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御手順と、をコンピュータに実行させることを特徴とする。

[0018] また、請求項11に係る発明は、上記の発明において、前記中継装置選択手順は、自己に隣接する複数の中継装置のなかから前記攻撃パケットによる攻撃を受けているサーバまたはドメインに対して次の中継先となる中継装置を除いて、前記経路情報の通知先となる中継装置を選択することを特徴とする。

[0019] また、請求項12に係る発明は、上記の発明において、自己と隣接関係をもつ他の防御装置に対して前記攻撃情報を送信する攻撃情報送信手順をさらにコンピュータに実行させ、前記中継装置選択手順は、前記他の防御装置から前記攻撃情報を受信した場合にも、当該攻撃情報に基づいて前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択することを特徴とする。

[0020] また、請求項13に係る発明は、上記の発明において、前記経路情報通知手順によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットを監視して、当該中継装置から自己に経由される攻撃パケットの送信が終了したか否かを判定する攻撃終了判定手順をさらにコンピュータに実行させ、前記経路情報通

知手順は、前記攻撃終了判定手順によって前記攻撃パケットの送信が終了したものと判定された場合に、当該攻撃パケットを自己に経由させないための経路情報を前記中継装置に通知することを特徴とする。

発明の効果

[0021] 請求項1、5、6または10の発明によれば、攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置を攻撃パケットの流入方向も考慮して選択し、当該選択した中継装置から自己に経由されてきた攻撃パケットの通過を制御するので、攻撃パケットの流入方向に影響されることなく攻撃パケットを防御することが可能になる。

[0022] また、請求項2、7または11の発明によれば、攻撃を受けているサーバまたはドメインに対して次の中継先となる中継装置を除いた他の中継装置に経路情報を通知し、後者の中継装置から自己に経由されてきたパケットを前者の中継装置に中継するので、パケットのループを防止することが可能になる。

[0023] また、請求項3、8または12の発明によれば、自己と隣接関係をもつ他の防御装置に対して攻撃情報を送信するとともに、他の防御装置から攻撃情報を受信した場合にも、当該攻撃情報に基づいて攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置を選択し、当該選択した中継装置から自己に経由されてきた攻撃パケットの通過を制御するので、攻撃発生元に近い防御装置において攻撃を防御することが可能になる。

[0024] また、請求項4、9または13の発明によれば、中継装置から自己に経由される攻撃パケットの送信が終了した場合に、攻撃パケットを自己に経由させないための経路情報を中継装置に改めて通知するので、防御装置を経由する攻撃パケットの迂回を効率的に切替えることが可能になる。

図面の簡単な説明

[0025] [図1]図1は、実施例1に係るネットワーク攻撃防御システムの構成を示す図である。

[図2]図2は、実施例1における防御装置の構成を示すブロック図である。

[図3]図3は、容疑シグネチャの例を示す図である。

[図4]図4は、正規条件情報の例を示す図である。

[図5]図5は、不正トラヒック検出条件の例を示す図である。

[図6]図6は、攻撃情報受信時の処理手順を示すフローチャートである。

[図7]図7は、不正パケット検出時の処理手順を示すフローチャートである。

[図8]図8は、パケット制御時の処理手順を示すフローチャートである。

[図9]図9は、実施例2に係るネットワーク攻撃防御システムの構成を示す図である。

[図10]図10は、実施例2における防御装置の構成を示すブロック図である。

[図11]図11は、攻撃情報受信時の処理手順を示すフローチャートである。

[図12]図12は、攻撃終了判定の処理手順を示すフローチャートである。

[図13]図13は、従来技術に係るネットワーク攻撃防御システムを説明するための図である。

符号の説明

[0026] 10、60 防御装置

11 ネットワークインタフェース部

12 パケット制御部

13、63 攻撃情報処理部

14 中継装置選択部

15 経路情報通知部

16 パケット取得部

17、67 攻撃検出部

20 サーバ

30 中継装置

40 通信端末

50 検知装置

83 ルータ

95 攻撃検知装置

100、200 ネットワーク攻撃防御システム

発明を実施するための最良の形態

[0027] 以下に添付図面を参照して、この発明に係る防御装置、防御方法および防御プロ

グラム並びにネットワーク攻撃防御システムの実施例を詳細に説明する。なお、以下では、一つの防御装置で攻撃を防御するネットワーク攻撃防御システムを実施例1として説明するとともに、複数の防御装置で攻撃を防御するネットワーク攻撃防御システムを実施例2として説明し、最後に、実施例1および2に対する種々の変形例を実施例3として説明する。

実施例 1

[0028] 以下の実施例1では、一つの防御装置で攻撃を防御するネットワーク攻撃防御システムについて、システムの概要および特徴を説明した後に、防御装置の構成および処理、実施例1の効果を順に説明する。

[0029] [システムの概要および特徴(実施例1)]

最初に、図1を用いて、実施例1に係るネットワーク攻撃防御システムの概要および特徴を説明する。図1は、実施例1に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[0030] 同図に示すように、このネットワーク攻撃防御システム100は、ネットワーク上のサーバ20に対するDoS攻撃またはDDoS攻撃が検出された場合に、この攻撃を防御する防御装置10と、サーバ20に送信されるパケットを中継する複数の中継装置30とをネットワーク上に備える。また、このネットワーク上には、サーバ20や通信端末40が接続されており、さらに、サーバ20が攻撃を受けたことを検知する検知装置50が設けられている。

[0031] なお、中継装置30は、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、以下の説明において、図示した中継装置30の各々を区別する場合には、中継装置30－1または中継装置30－2とし、サーバ20の各々を区別する場合には、サーバ20－1またはサーバ20－2として記載する。

[0032] かかるネットワーク攻撃防御システム100において、防御装置10および中継装置30には、パケットの宛先を規定したルーティング表が登録されている。なお、ルーティング表を登録する方法としては、例えば、OSPF(OpenShortestPathFirst)、RIP(RoutingInformationProtocol)またはBGP(BorderGatewayProtocol)などの公知のルーティングプロトコルに準拠して登録するようにしてもよい。

[0033] そして、通信端末40がサーバ20－1にパケットを通常に送信した場合には、この送信されたパケットは、中継装置30－1および中継装置30－2それぞれのルーティング表に従って、防御装置10を中継せずに中継装置30－2および中継装置30－1を介してサーバ20－1に中継される。

[0034] ここで、通信端末40が攻撃者であり、攻撃を行うための攻撃パケットをサーバ20－1に送信していた場合には、検知装置50は、サーバ20－1に対する攻撃を検出し、攻撃を検出した旨を示す攻撃情報を防御装置10に送信する(図1の(1)および(2)参照)。なお、この攻撃情報には、攻撃を受けているサーバ20－1のアドレス等が含まれる。また、検知装置50および防御装置10は、検知装置50および防御装置10等を管理するための管理用ネットワークに接続されていてもよく、攻撃情報は、管理用ネットワークを介して送受されてもよい。

[0035] 一方、検知装置50から送信された攻撃情報を受信した防御装置10は、受信した攻撃情報に基づいて、攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置30を選択する(同図の(3)参照)。ここで、実施例1に係るネットワーク攻撃防御システム100では、攻撃パケットの流入方向も考慮して中継装置を選択することで、攻撃パケットの流入方向に影響されることなく攻撃パケットを防御することができるようにしている点に主たる特徴がある。

[0036] すなわち、防御装置10は、攻撃情報から攻撃を受けているサーバ20を特定し、攻撃を受けているサーバ20のアドレスが含まれるパケットに対する次の中継先となる中継装置30をルーティング表から求め、防御装置10と隣接する複数の中継装置30のうち、次の中継先となる中継装置30を除く中継装置30を通知先として選択する。例えば、図1に示した例で言えば、攻撃情報から攻撃を受けているサーバ20－1を特定した場合には、特定したサーバ20－1に対して次の中継先となる中継装置30－1をルーティング表から求め、防御装置10と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－1を除いた中継装置30－2を通知先として選択する。

[0037] かかる中継装置30の選択後、防御装置10は、選択した中継装置30－2に対して、攻撃パケットを自己に経由させるための経路情報を通知し(同図の(4)参照)、中継

装置30－2は、通知された経路情報に基づいてルーティング表を変更する(同図の(5)参照)。この結果、中継装置30－2は、サーバ20－1行きの攻撃パケットを防御装置10に中継することになる。つまり、攻撃パケットは、中継装置30－2、防御装置10、中継装置30－1を介してサーバ20－1に中継される。

[0038] そして、防御装置10は、中継装置30－2から中継された攻撃パケットの通過を攻撃情報に基づいて制御しながら、サーバ20－1向けのパケットを中継する。仮に、攻撃の対象がサーバ20ではなく、あるドメインであった場合に、このドメイン行きの攻撃パケットが防御装置10に中継される。なお、防御装置10は、攻撃パケットを監視した上で、通信端末40からの攻撃が終了したと判断した場合には、サーバ20－1行きのパケットを自己に経由させないための経路情報を中継装置30－2に通知し、これを受信した中継装置30－2は、通知された経路情報に基づいてルーティング表を変更する。

[0039] [防御装置の構成(実施例1)]

次に、図2を用いて、図1に示した防御装置10の構成を説明する。図2は、実施例1における防御装置10の構成を示すブロック図である。同図に示すように、この防御装置10は、ネットワークインタフェース部11と、パケット制御部12と、攻撃情報処理部13と、中継装置選択部14と、経路情報通知部15と、パケット取得部16と、攻撃検出部17とを備えて構成される。

[0040] ところで、防御装置10は、CPU(CentralProcessingUnit)やメモリ、ハードディスク等を有しており、パケット制御部12、攻撃情報処理部13、中継装置選択部14、経路情報通知部15、パケット取得部16および攻撃検出部17は、CPUによって処理されるプログラムのモジュールでもよい。また、このプログラムのモジュールは、1つのCPUで処理されてもよく、複数のCPUに分散して処理されてもよい。

[0041] なお、パケット制御部12は特許請求の範囲に記載の「パケット制御手段」に対応し、中継装置選択部14は同じく「中継装置選択手段」に対応し、経路情報通知部15は同じく「経路情報通知手段」に対応する。

[0042] 図2において、ネットワークインタフェース11は、ネットワークと接続されている通信機器との間でパケットや攻撃情報等を送受信する手段であり、具体的には、LAN(L

ocalAreaNetwork)またはWAN(WideAreaNetwork)などのネットワークと接続するためのネットワーク接続カード等によって構成される。

[0043] パケット制御部12は、パケットの宛先に対するルーティング表が登録されており、ルーティング表に従って、受信したパケットを中継する処理部である。また、パケット制御部12は、パケットフィルタリングを行う図示しないフィルタ部を有し、ネットワークインタフェース部11が受信したパケットの通過を制御し、通過させるパケットをネットワークインタフェース部11に出力する処理部でもある。なお、かかるパケットフィルタリングについては後に図8を用いて詳述する。

[0044] 攻撃情報処理部13は、検知装置50がDoS攻撃またはDDoS攻撃を検出した場合に、攻撃を検出した旨を示す攻撃情報を受信する処理部である。ここで、攻撃情報には、攻撃を受けているサーバ20のアドレスに加えて、パケットの通過を制御するためのシグネチャ等が含まれるようにしてもよい。すなわち、攻撃情報処理部13が、攻撃に対して容疑のかかるパケットとなる容疑パケットを制限するための容疑シグネチャや正規条件情報も受信するようにしてもよい。

[0045] ここで、図3を用いて、容疑シグネチャについて説明する。図3は、容疑シグネチャの例を示す図である。同図に示すように、容疑シグネチャは、容疑パケットの検出条件を表す情報によって構成される。具体的には、例えば、同図に例示した番号1の容疑シグネチャは、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.1/32」であり(dst=192.168.1.1/32)、IPの上位層(TCPまたはUDP)のプロトコル種別を示す「Protocol(プロトコル)」が「TCP」であり(Protocol=TCP)、かつ、IPの上位層プロトコルがどのアプリケーションの情報であるかを示す「DestinationPort(宛先ポート番号)」が「80」である(Port=80)という検出属性の組合せで構成される。

[0046] また、同図に例示した番号2の容疑シグネチャは、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.2/32」であり(dst=192.168.1.2/32)、かつ、「Protocol(プロトコル)」が「UDP(UserDatagramprotocol)」である(Protocol=UDP)という検出属性の組合せで構成される。同様に、番号3の容疑シグネチャは、「DestinationIPAddress(宛先IPアドレス)」が「192.168.1.0/24」という検出属性の組合せで構成される。なお、攻撃情報処理部13が受信した容疑シグネチャは、上記したパケット制御部12のフィ

ルタ部に登録され、パケット通過の制御に用いられる。

[0047] 続いて、図4を用いて、攻撃情報処理部13が受信する正規条件情報、すなわち、正当な利用者が利用している端末から送信されるパケットを表す正規条件情報について説明する。図4は、正規条件情報の例を示す図である。同図に示すように、正規条件情報は、IPパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0048] 具体的には、番号1のレコードの検出属性は、IPの「SourceIPAddress(送信元IPアドレス)」が「172.16.10.0/24」であることを指定し(src=172.16.10.0/24)、番号2のレコードの検出属性はIP上のサービス品質を示す「TypeofService(サービスタイプ)」が「(16進で)01」であることを指定している(TOS=0x01)。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ20等の送信元IPアドレスが設定され、サーバ20が収容されているLANの所有者が正規ユーザであると認識しているネットワークの送信元IPアドレスなどが設定される。なお、後述する攻撃検出部17は、かかる正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのAND条件をとり、これを正規シグネチャとして生成する。

[0049] 図2において、中継装置選択部14は、攻撃情報処理部13によって受信された攻撃情報に基づいてネットワーク上にある複数の中継装置30のなかから攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置30を選択する処理部である。具体的には、中継装置選択部14は、攻撃情報から攻撃を受けているサーバ20を特定し、攻撃を受けているサーバ20のアドレスが含まれるパケットに対する次の中継先となる中継装置30をルーティング表から求め、防御装置10と隣接する複数の中継装置30のうち、次の中継先となる中継装置30を除く中継装置30を通知先として選択する。

[0050] 例えば、図1に示した例で言えば、攻撃情報から攻撃を受けているサーバ20－1を特定した場合には、特定したサーバ20－1行きのパケットに対して次の中継先となる中継装置30－1をルーティング表から求め、防御装置10と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－1を除いた中継装置30－2を

通知先として選択する。一方、図1において、サーバ20－2から攻撃を受けている通信端末40を特定したような場合には、特定した通信端末40行きのパケットに対して次の中継先となる中継装置30－2をルーティング表から求め、防御装置10と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－2を除いた中継装置30－1を通知先として選択する。

[0051] 経路情報通知部15は、攻撃を受けている対象に送信されるパケットを防御装置10に経由させるための経路情報を、中継装置選択部14によって選択された中継装置30に通知する処理部である。具体的には、上記した例で言えば、攻撃情報から攻撃を受けているサーバ20－1を特定した場合には、中継装置30－2に対して、サーバ20－1に送信されるパケットを防御装置10に経由させるための経路情報を送信する。なお、この経路情報には、攻撃を受けている対象のIPアドレスやネットワークアドレス等が含まれる。また、例えば、経路情報通知部15は、BGPに準拠して、選択された中継装置30に経路情報を通知するようにしてもよい。

[0052] パケット取得部16は、ネットワークインタフェース部11が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部17等に提供する処理部である。

[0053] 攻撃検出部17は、パケット取得部16によって提供された統計情報および攻撃情報処理部13によって受信した攻撃情報に基づいて、攻撃の検出や分析を行い、さらには、正規シグネチャや不正シグネチャの生成を行う処理部である。

[0054] ここで、正規シグネチャの生成を具体的に説明すると、攻撃情報処理部13が攻撃情報（容疑シグネチャおよび正規条件情報を含む。）を受信した場合に、攻撃検出部17は、図4に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのAND条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケットを許可するために用いられるシグネチャであるが、例えば、図3および図4の例を用いて説明すると、図3における番号1のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32,Protocol=TCP,Port=80]となり、図4において、正規シグネチャは、[src=172.16.10.24,dst=192.168.1.1/32,Protocol=TCP,Port=80]および[TOS=0x01,dst

=192.168.1.1/32,Protocol=TCP,Port=80]となる。

[0055] また、攻撃検出部17が不正なトラヒックを検出するようにしてもよく、その場合には、攻撃検出部17は、不正なトラヒックを検出するための不正トラヒック検出条件を保有する。ここで、図5を用いて、不正トラヒック検出条件を説明する。図5は、不正トラヒック検出条件の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のDDoS攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。なお、番号はレコード(パターン)を特定するために便宜上使用されるものである。

[0056] 具体的には、番号1の不正トラヒック条件は、「伝送帯域T1Kbps以上のパケットがS1秒以上連続送信されている」というトラヒックパターンを示している。また、番号2の不正トラヒック条件は、「伝送帯域T2Kbps以上、ICMP(InternetControlMessageProtocol)上のエコー応答(EchoReply)メッセージのパケットがS2秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号3の不正トラヒック条件は、「伝送帯域T3Kbps以上、データが長すぎるためパケットに含まれるデータは複数IPパケットに分割して送信していることを示すフラグメントパケットがS3秒以上連続送信されている」というトラヒックパターンを示している。

[0057] そして、攻撃検出部17は、図4に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元IPアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

[0058] なお、上述してきた攻撃検出部17によって生成された正規シグネチャおよび不正シグネチャは、攻撃情報処理部13によって受信された容疑シグネチャと同様、上記したパケット制御部12のフィルタ部に登録され、パケット通過の制御に用いられる。

[0059] [攻撃情報受信時の処理(実施例1)]

続いて、図6を参照して、上記した防御装置10による攻撃情報受信時の動作処理を説明する。図6は、攻撃情報受信時の処理手順を示すフローチャートである。

[0060] 同図に示すように、防御装置10の攻撃情報処理部13が、検知装置50から送信さ

れた攻撃情報を受信すると(ステップS1)、中継装置選択部14は、受信された攻撃情報に基づいて、攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置30を選択する(ステップS2)。

[0061] 具体的には、中継装置選択部14は、図1に示した例で言えば、攻撃情報に基づいて攻撃を受けているサーバ20－1を特定した後に、特定したサーバ20－1行きのパケットに対して次の中継先となる中継装置30－1をルーティング表から求め、防御装置10と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－1を除いた中継装置30－2を通知先として選択する。

[0062] その後、防御装置10の経路情報通知部15は、中継装置選択部14によってステップS2で選択された中継装置30に対して、攻撃を受けている対象に送信されるパケットを防御装置10に経由させるための経路情報を通知する(ステップS3)。具体的には、上記した例で言えば、中継装置30－2に対して、サーバ20－1に送信されるパケットを防御装置10に経由させるための経路情報を送信する。

[0063] そして、攻撃検出部17は、攻撃情報に含まれていた容疑シグネチャおよび正規条件情報に基づいて正規シグネチャを生成し(ステップS4)、さらに、攻撃情報に含まれていた容疑シグネチャおよびステップS4で生成した正規シグネチャをパケット制御部12(フィルタ部)に登録する(ステップS5)。

[0064] 上述したステップS3の処理によって経路情報を受信した中継装置30－2は、通知された経路情報に基づいてルーティング表を変更し、その結果、中継装置30－2は、サーバ20－1行きの攻撃パケットを防御装置10に中継する。そして、防御装置10は、中継装置30－2から中継された攻撃パケットの通過を攻撃情報に基づいて制御しながらサーバ20－1向けのパケットを中継する。

[0065] [不正パケット検出時の処理(実施例1)]

続いて、図7を参照して、上記した防御装置10による不正パケット検出時の動作処理を説明する。図7は、不正パケット検出時の処理手順を示すフローチャートである。

[0066] 同図に示すように、防御装置10の攻撃検出部17が、図5に示した不正トラヒック条件に基づいて不正トラヒックを検出すると(ステップS11)、不正シグネチャを生成する(ステップS12)。そして、攻撃検出部17は、生成した不正シグネチャをパケット制御

部12(フィルタ部)に登録する(ステップS13)。

[0067] [パケット制御時の処理(実施例1)]

続いて、図8を参照して、上記した防御装置10によるパケット制御時の動作処理を説明する。図8は、パケット制御時の処理手順を示すフローチャートである。

[0068] 同図に示すように、パケット制御部12(フィルタ部)は、ネットワークインタフェース11からパケットが入力されると(ステップS21肯定)、登録された不正シグネチャに合致するか否かを判断する(ステップS22)。そして、不正シグネチャに合致した場合には(ステップS22肯定)、パケット制御部12は、不正なパケットを処理するための不正キューにパケットを入力する(ステップS23)。

[0069] これとは反対に、不正シグネチャに合致しない場合には(ステップS22否定)、パケット制御部12は、入力されたパケットが、登録された正規シグネチャに合致するか否かを判断する(ステップS24)。そして、正規シグネチャに合致した場合には(ステップS24肯定)、パケット制御部12は、正規なユーザ用の正規キューにパケットを入力する(ステップS25)。

[0070] さらに、この正規シグネチャにも合致しない場合には(ステップS24否定)、パケット制御部12は、入力されたパケットが、登録された容疑シグネチャに合致するか否かを判断する(ステップS26)。そして、容疑シグネチャに合致した場合には(ステップS26肯定)、パケット制御部12は、容疑ユーザ用の容疑キューにパケットを入力する(ステップS27)。これとは反対に、容疑シグネチャに合致しない場合には(ステップS26否定)、パケット制御部12は、正規キューにパケットを入力する(ステップS28)。

[0071] そして、パケット制御部12は、それぞれのキューにあるパケットについて、正規キューであれば、伝送帯域を制限せずにネットワークインタフェース部11から出力し、容疑キューおよび不正キューであれば、それぞれのシグネチャが示す伝送帯域制限値に従って制限して出力する。なお、不正シグネチャ、正規シグネチャ、容疑シグネチャの各シグネチャは、パケット制御部12(フィルタ部)に複数登録されてもよい。また、登録されたシグネチャの検出属性等が所定の判断基準を満たした場合に、パケット制御部12は、所定の判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいたパケットの通過を制御する処理を停止する。

[0072] [実施例1の効果]

上述してきたように、上記の実施例1によれば、攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置30を攻撃パケットの流入方向も考慮して選択し、当該選択した中継装置30から自己に経由されてきた攻撃パケットの通過を制御するので、攻撃パケットの流入方向に影響されることなく攻撃パケットを防御することが可能になる。

[0073] また、上記の実施例1によれば、攻撃を受けているサーバ20－1(またはドメイン)に対して次の中継先となる中継装置30－1を除いた他の中継装置30－2に経路情報を通知し、後者の中継装置30－2から自己に経由されてきたパケットを前者の中継装置30－2に中継するので、パケットのループを防止することが可能になる。

実施例 2

[0074] 次に、以下の実施例2では、複数の防御装置で攻撃を防御するネットワーク攻撃防御システムについて、システムの概要および特徴を説明した後に、防御装置の構成および処理、実施例2の効果を順に説明する。

[0075] [システムの概要および特徴(実施例2)]

最初に、図9を用いて、実施例2に係るネットワーク攻撃防御システムの概要および特徴を説明する。図9は、実施例2に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

[0076] 同図に示すように、このネットワーク攻撃防御システム200は、ネットワーク上のサーバ20に対するDoS攻撃またはDDoS攻撃が検出された場合に、この攻撃を防御する防御装置60と、サーバ20に送信されるパケットを中継する複数の中継装置30とをネットワーク上に備える。また、このネットワーク上には、サーバ20や通信端末40が接続されており、さらに、サーバ20が攻撃を受けたことを検知する検知装置50が設けられている。

[0077] なお、実施例2に係るネットワーク攻撃防御システム200を構成する構成要素のうち、上記した実施例1に係るネットワーク攻撃防御システム100を構成する構成要素と同一の構成要素には同一の符号を付し、それぞれの説明を省略する。また、以下の説明において、図示した中継装置30の各々を区別する場合には、中継装置30－1

または中継装置30－2とし、サーバ20の各々を区別する場合には、サーバ20－1またはサーバ20－2として記載する。また、防御装置60の各々を区別する場合には、防御装置60－1または防御装置60－2とし、通信端末40の各々を区別する場合には、通信端末40－1または通信端末40－2として記載する。

[0078] かかるネットワーク攻撃防御システム200において、防御装置60および中継装置30には、パケットの宛先を規定したルーティング表が登録されている。なお、ルーティング表を登録する方法としては、例えば、OSPF、RIPまたはBGPなどの公知のルーティングプロトコルに準拠して登録するようにしてもよい。

[0079] そして、通信端末40－1がサーバ20－1にパケットを通常に送信した場合には、この送信されたパケットは、中継装置30－1～中継装置30－3それぞれのルーティング表に従って、防御装置60を中継せずに中継装置30－3、中継装置30－2、中継装置30－1を介してサーバ20－1に中継される。

[0080] ここで、通信端末40－1が攻撃者であり、攻撃を行うための攻撃パケットをサーバ20－1に送信していた場合には、検知装置50は、サーバ20－1に対する攻撃を検出し、攻撃を検出した旨を示す攻撃情報を防御装置60－1に送信する(図9の(1)および(2)参照)。なお、防御装置60は、防御装置60等を管理するための管理用ネットワークに接続されていてもよく、攻撃情報は、管理用ネットワークを介して送受されてもよい。

[0081] 一方、検知装置50から送信された攻撃情報を受信した防御装置60－1は、受信した攻撃情報に基づいて、攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置30を選択する(同図の(3)参照)。具体的には、上記した実施例1と同様、攻撃情報から攻撃を受けているサーバ20－1を特定した上で、特定したサーバ20－1行きのパケットに対して次の中継先となる中継装置30－1をルーティング表から求め、防御装置60－1と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－1を除いた中継装置30－2を通知先として選択する。

[0082] かかる中継装置30の選択後、防御装置60－1は、選択した中継装置30－2に対して、攻撃パケットを自己に経由させるための経路情報を通知し(同図の(4)参照)、中継装置30－2は、通知された経路情報に基づいてルーティング表を変更する(同

図の(5)参照)。この結果、中継装置30－2は、サーバ20－1行きの攻撃パケットを防御装置60－1に中継することになる。つまり、攻撃パケットは、中継装置30－3、中継装置30－2、防御装置60－1、中継装置30－1を介してサーバ20－1に中継される。そして、防御装置60－1は、中継装置30－2から中継された攻撃パケットの通過を攻撃情報に基づいて制御しながら、サーバ20－1向けのパケットを中継する。

[0083] このようにして、中継装置30－2のルーティング表が変更され、攻撃パケットが中継装置30－2から防御装置60－1に中継されて処理されることになるが、実施例2に係るネットワーク攻撃防御システム200の防御装置60では、攻撃情報に基づいて所定の中継装置30を選択してルーティング表を変更させるだけでなく、隣接関係をもつ他の防御装置60に対して攻撃情報を送信する点にも主たる特徴がある。

[0084] すなわち、防御装置60－1は、経路情報を中継装置30－2に通知した後、防御装置60－1と隣接関係をもつ防御装置60－2に対して攻撃情報を送信する(同図の(6)参照)。その結果、攻撃情報を受信した防御装置60－2も、防御装置60－1と同様、攻撃情報に基づいて、攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置30を選択する(同図の(7)参照)。具体的には、受信した攻撃情報から攻撃を受けているサーバ20－1を特定し、特定したサーバ20－1行きのパケットに対して次の中継先となる中継装置30－2をルーティング表から求め、防御装置60－2と隣接する中継装置30－2および中継装置30－3のなかから、この中継装置30－2を除いた中継装置30－3を選択する。

[0085] かかる中継装置30の選択後、防御装置60－2は、選択した中継装置30－3に対して、攻撃パケットを自己に経由させるための経路情報を通知し(同図の(8)参照)、中継装置30－3は、通知された経路情報に基づいてルーティング表を変更する(同図の(9)参照)。この結果、中継装置30－3は、サーバ20－1行きの攻撃パケットを防御装置60－2に中継することになる。つまり、攻撃パケットは、中継装置30－3、防御装置60－2、中継装置30－2、防御装置60－1、中継装置30－1を介してサーバ20－1に中継される。そして、防御装置60－2は、中継された攻撃パケットの通過を攻撃情報に基づいて制御しながら、サーバ20－1向けのパケットを中継するようになっている。

[0086] このようにして、中継装置30－1よりも攻撃元に近い中継装置30－3のルーティング表が変更され、攻撃パケットが中継装置30－3から防御装置60－2に中継されて処理されることになるが、実施例2に係るネットワーク攻撃防御システム200の防御装置60では、隣接関係をもつ他の防御装置60に対して攻撃情報を送信するだけでなく、先にルーティング表を変更した中継装置30による自己へのパケット中継を解除する点にも主たる特徴がある。

[0087] すなわち、防御装置60－2は、隣接関係をもつ他の防御装置60に対して攻撃情報を送信した後に、自己に対する攻撃パケットの送信が終了したか否かを判定する(同図の(10)参照)。具体的には、上記した例で言えば、防御装置60－2が攻撃パケットの通過を制御することによって、攻撃パケットが防御装置60－1を一定期間通過しなくなった場合には、防御装置60－1は、通信端末40－1からの攻撃が終了したと判断する。

[0088] その上で、防御装置60－1は、サーバ20－1行きのパケットを自己に経由させないための経路情報を、先にルーティング表を変更した中継装置30－2に通知し(同図の(11)参照)、中継装置30－2は、通知された経路情報に基づいてルーティング表を変更する(同図の(12)参照)。この結果、中継装置30－2は、サーバ20－1行きの攻撃パケットを防御装置60－1ではなく中継装置30－1に中継することになる。つまり、攻撃パケットは、中継装置30－3、防御装置60－2、中継装置30－2、中継装置30－1を介してサーバ20－1に中継される。

[0089] [防御装置の構成(実施例2)]

次に、図10を用いて、図9に示した防御装置60の構成を説明する。図10は、実施例2における防御装置60の構成を示すブロック図である。同図に示すように、この防御装置60は、ネットワークインタフェース部11と、パケット制御部12と、攻撃情報処理部63と、中継装置選択部14と、経路情報通知部15と、パケット取得部16と、攻撃検出部67とを備えて構成される。

[0090] ここで、パケット制御部12は特許請求の範囲に記載の「パケット制御手段」に対応し、攻撃情報処理部63は同じく「攻撃情報送信手段」に対応し、中継装置選択部14は同じく「中継装置選択手段」に対応し、経路情報通知部15は同じく「経路情報通知手

段」に対応し、攻撃検出部67は同じく「攻撃終了判定手段」に対応する。以下、実施例2における防御装置60を構成する構成要素のうち、上記した実施例1における防御装置10を構成する構成要素と同一の構成要素には同一の符号を付し、それぞれの説明を省略する。

[0091] 図10において、攻撃情報処理部63は、検知装置50がDoS攻撃またはDDoS攻撃を検出した場合に、攻撃を検出した旨を示す攻撃情報を受信することに加えて、受信した攻撃情報を自己の防御装置60と隣接関係をもつ防御装置60である隣接防御装置に送信する処理部である。ただし、攻撃情報を自己の防御装置60に送信した隣接中継装置には、攻撃情報処理部63は攻撃情報を送信しない。例えば、図9に示したネットワーク攻撃防御システム200において、防御装置60－1が攻撃情報を防御装置60－2に送信したような場合には、防御装置60－2の攻撃情報処理部63は、攻撃情報を送信した隣接中継装置である防御装置60－1に再度、攻撃情報を送信することはない。

[0092] 攻撃検出部67は、パケット取得部16によって提供された統計情報および攻撃情報処理部13によって提供された攻撃情報に基づいて、攻撃の検出や分析を行うことや、正規シグネチャや不正シグネチャの生成を行うことに加えて、攻撃が終了したか否かを判断する処理部である。具体的には、隣接関係をもつ他の防御装置60に対して攻撃情報を送信した後に、自己に対する攻撃パケットの送信が終了したか否かを判定するが、図9に示した例で言えば、防御装置60－2が攻撃パケットの通過を制御することによって、攻撃パケットが防御装置60－1を一定期間通過しなくなった場合には、防御装置60－1の攻撃検出部67は、通信端末40－1からの攻撃が終了したと判断する。

[0093] また、経路情報通知部15は、攻撃を受けている対象に送信されるパケットを自己に経由させるための経路情報を、中継装置選択部14によって選択された中継装置30に通知することに加えて、上記の攻撃検出部67によって攻撃が終了したと判定された場合には、攻撃を受けている対象に送信されるパケットを自己に経由させないための経路情報を、先に中継装置選択部14によって選択された中継装置30に通知する。

[0094] [攻撃情報受信時の処理(実施例2)]

続いて、図11を参照して、上記した防御装置60による攻撃情報受信時の動作処理を説明する。図11は、攻撃情報受信時の処理手順を示すフローチャートである。

[0095] 同図に示すように、防御装置60の攻撃情報処理部63が、検知装置50から送信された攻撃情報、または、他の隣接する防御装置60から送信された攻撃情報を受信すると(ステップS31)、中継装置選択部14は、受信された攻撃情報に基づいて、攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置30を選択する(ステップS32)。

[0096] 具体的には、図9に示した例で言えば、防御装置60－1が検知装置50から攻撃情報を受信した場合には、攻撃情報に基づいて攻撃を受けているサーバ20－1を特定した後に、特定したサーバ20－1行きのパケットに対して次の中継先となる中継装置30－1をルーティング表から求め、防御装置60－1と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－1を除いた中継装置30－2を通知先として選択する。

[0097] その一方、防御装置60－2が防御装置60－1から攻撃情報を受信した場合には、攻撃情報に基づいて攻撃を受けているサーバ20－1を特定した後に、特定したサーバ20－1行きのパケットに対して次の中継先となる中継装置30－2をルーティング表から求め、防御装置60－2と隣接する中継装置30－2および中継装置30－3のなかから、この中継装置30－2を除いた中継装置30－3を通知先として選択する。

[0098] その後、防御装置60の経路情報通知部15は、中継装置選択部14によってステップS32で選択された中継装置30に対して、攻撃を受けている対象に送信されるパケットを自己に経由させるための経路情報を通知する(ステップS33)。具体的には、上記した例で言えば、防御装置60－1は、中継装置30－2に対して、サーバ20－1に送信されるパケットを防御装置60－1に経由させるための経路情報を送信し、防御装置60－2は、中継装置30－3に対して、サーバ20－1に送信されるパケットを防御装置60－2に経由させるための経路情報を送信する。

[0099] そして、防御装置60の攻撃検出部67は、攻撃情報に含まれていた容疑シグネチャおよび正規条件情報に基づいて正規シグネチャを生成し(ステップS34)、さらに、

攻撃情報に含まれていた容疑シグネチャおよびステップS34で生成した正規シグネチャをパケット制御部12(フィルタ部)に登録する(ステップS35)。

[0100] さらに、防御装置60の攻撃情報処理部63は、自己に隣接する防御装置60の有無を判定し(ステップS36)、隣接する防御装置60が有る場合には(ステップS36肯定)、上記のステップS31で受信した攻撃情報を隣接防御装置に送信する(ステップS37)。具体的には、上記した例で言えば、防御装置60－1は、隣接する防御装置60－2があるので、この防御装置60－2に対して攻撃情報を送信するが、防御装置60－2は、隣接する防御装置60がないので、攻撃情報の送信は行わない。

[0101] 上述したステップS33の処理によって経路情報を受信した中継装置30－2や中継装置30－3は、通知された経路情報に基づいてルーティング表を変更し、その結果、中継装置30－2は、サーバ20－1行きの攻撃パケットを防御装置60－1に中継し、また、中継装置30－3は、サーバ20－1行きの攻撃パケットを防御装置60－2に中継する。そして、防御装置60－1および防御装置60－2は、中継装置30－2や中継装置30－3から中継された攻撃パケットの通過を攻撃情報に基づいて制御しながらサーバ20－1向けのパケットを中継する。

[0102] [攻撃終了判定の処理(実施例2)]

続いて、図12を参照して、上記した防御装置60による攻撃終了判定の動作処理を説明する。図12は、攻撃終了判定の処理手順を示すフローチャートである。

[0103] 同図に示すように、防御装置60の攻撃検出部67は、自己に対する攻撃パケットの送信が終了したか否かを判定する(ステップS41)。具体的には、図9に示した例で言えば、防御装置60－2が攻撃パケットの通過を制御することによって、攻撃パケットが防御装置60－1を一定期間通過しなくなった場合には、防御装置60－1の攻撃検出部67は、通信端末40－1からの攻撃が終了したと判断する。

[0104] そして、防御装置60の経路情報通知部15は、攻撃を受けている対象に送信されるパケットを自己に経由させるための経路情報を、図11のステップS32で選択された中継装置30に対して通知する(ステップS42)。具体的には、図9に示した例で言えば、防御装置60－1は、サーバ20－1行きのパケットを自己に経由させないための経路情報を、先にルーティング表を変更した中継装置30－2に通知する。

[0105] これに続いて、パケット制御部12(フィルタ部)は、登録していた容疑シグネチャおよび正規シグネチャ等を解除し、解除されたシグネチャに基づいたパケットの通過を制御するための処理を停止する(ステップS43)。つまり、サーバ20－1行きの攻撃パケットを制御するために登録されていた容疑シグネチャや正規シグネチャ等を削除する。

[0106] 上述したステップS42の処理によって経路情報を受信した中継装置30－2は、通知された経路情報に基づいてルーティング表を変更し、その結果、中継装置30－2は、サーバ20－1行きの攻撃パケットを防御装置60－1ではなく、中継装置30－1に中継する。このため、通信端末40－1から送信されている攻撃パケットは、中継装置30－3、防御装置60－2、中継装置30－2、中継装置30－1を介してサーバ20－1に中継される。

[0107] なお、図12に示したステップS41の動作が開始されるタイミングは、防御装置60に経由させるための経路情報を中継装置30に通知した後の任意の時点、例えば、図11に示したステップS33の後などであることが望ましい。

[0108] [実施例2の効果]

上述してきたように、上記の実施例2によれば、自己(防御装置60)と隣接関係をもつ他の防御装置60に対して攻撃情報を送信するとともに、他の防御装置60から攻撃情報を受信した場合にも、当該攻撃情報に基づいて攻撃パケットを自己に経由させるための経路情報の通知先となる中継装置30を選択し、当該選択した中継装置30から自己に経由されてきた攻撃パケットの通過を制御するので、攻撃発生元に近い防御装置60において攻撃を防御することが可能になる。

[0109] また、上記の実施例2によれば、中継装置30から自己に経由される攻撃パケットの送信が終了した場合に、攻撃パケットを自己に経由させないための経路情報を中継装置30に改めて通知するので、防御装置60を経由する攻撃パケットの迂回を効率的に切替えることが可能になる。

実施例 3

[0110] さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。そこで、以下では実施例

3に係るネットワーク攻撃防御システムとして、種々の異なる実施例を説明する。

[0111] 例えば、上記の実施例では、防御装置10(または60)と隣接する複数の中継装置30のなかから一つの中継装置30を選択する例を説明したが、本発明はこれに限定されるものではなく、例えば、攻撃を受けているサーバ20に対して次の中継先となる中継装置30に複数の中継装置30が接続されているような場合には、当該複数の中継装置30を経路情報の通知先として選択するようにしてもよい。

[0112] また、上記の実施例で図示した各装置(例えば、図2や図10に例示した防御装置10や防御装置60)の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、防御装置10や防御装置60の分散・統合の具体的形態は図示のものに限られず、防御装置10や防御装置60の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、防御装置10や防御装置60にて行なわれる各処理機能は、その全部または任意の一部が、CPUおよび当該CPUにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0113] また、上記の実施例で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報(例えば、図3に例示した容疑シグネチャ、図4に例示した正規条件情報、図5に例示した不正トラヒック条件等)については、特記する場合を除いて任意に変更することができる。

[0114] また、上記の実施例では、不正シグネチャ、正規シグネチャおよび容疑シグネチャの3種類に分類されたシグネチャを利用することによってパケットの迂回を行う例を説明したが、本発明はこれに限定されるものではなく、例えば、単一のシグネチャを利用したり、3種類以外の種類数に分類されたシグネチャを利用したりすることによって迂回を行うこととしてもよい。また、シグネチャ自体を利用することなく、例えば、迂回を指示する指示情報などを用いてパケットの迂回を行うこととしてもよい。

[0115] なお、上記の実施例では、本発明を実現する各装置（例えば、防御装置10や防御装置60）を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。すなわち、実施例1や2で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク（FD）、CD－ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例1に示したような防御装置用プログラムを格納したCD－ROMを配布し、このCD－ROMに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

産業上の利用可能性

[0116] 以上のように、本発明に係る防御装置、防御方法および防御プログラム並びにネットワーク攻撃防御システムは、ネットワーク上のサーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して攻撃パケットの通過を制御する場合に有用であり、特に、攻撃パケットの流入方向に影響されることなく攻撃パケットを防御することなどに適する。

請求の範囲

[1] ネットワーク上のサーバまたはドメインに対する攻撃情報に基づいて、当該サーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御装置であって、

前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択手段と、

前記中継装置選択手段によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知手段と、

前記経路情報通知手段によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御手段と、

を備えたことを特徴とする防御装置。

[2] 前記中継装置選択手段は、自己に隣接する複数の中継装置のなかから前記攻撃パケットによる攻撃を受けているサーバまたはドメインに対して次の中継先となる中継装置を除いて、前記経路情報の通知先となる中継装置を選択することを特徴とする請求項1に記載の防御装置。

[3] 自己と隣接関係をもつ他の防御装置に対して前記攻撃情報を送信する攻撃情報送信手段をさらに備え、

前記中継装置選択手段は、前記他の防御装置から前記攻撃情報を受信した場合にも、当該攻撃情報に基づいて前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択することを特徴とする請求項1または2に記載の防御装置。

[4] 前記経路情報通知手段によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットを監視して、当該中継装置から自己に経由される攻撃パケットの送信が終了したか否かを判定する攻撃終了判定手段をさらに備え、

前記経路情報通知手段は、前記攻撃終了判定手段によって前記攻撃パケットの送信が終了したものと判定された場合に、当該攻撃パケットを自己に経由させないための経路情報を前記中継装置に通知することを特徴とする請求項1に記載の防御装置

。

[5] ネットワーク上のサーバまたはドメインに送信されるパケットを中継する複数の中継装置と、当該サーバまたはドメインに対する攻撃情報に基づいて所定の中継装置に対して経路情報を送信し、当該サーバまたはドメイン宛の攻撃パケットの通過を制御する防御装置とを有するネットワーク攻撃防御システムであって、

前記防御装置は、

前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択手段と、

前記中継装置選択手段によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知手段と、

前記経路情報通知手段によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御手段と、

を備えたことを特徴とするネットワーク攻撃防御システム。

[6] ネットワーク上のサーバまたはドメインに対する攻撃情報に基づいて、当該サーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御装置による防御方法であって、

前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択工程と、

前記中継装置選択工程によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知工程と、

前記経路情報通知工程によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御工程と、

を含んだことを特徴とする防御方法。

[7] 前記中継装置選択工程は、自己に隣接する複数の中継装置のなかから前記攻撃パケットによる攻撃を受けているサーバまたはドメインに対して次の中継先となる中継装置を除いて、前記経路情報の通知先となる中継装置を選択することを特徴とする

請求項6に記載の防御方法。

[8] 自己と隣接関係をもつ他の防御装置に対して前記攻撃情報を送信する攻撃情報送信工程をさらに含み、

前記中継装置選択工程は、前記他の防御装置から前記攻撃情報を受信した場合にも、当該攻撃情報に基づいて前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択することを特徴とする請求項6または7に記載の防御方法。

[9] 前記経路情報通知工程によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットを監視して、当該中継装置から自己に経由される攻撃パケットの送信が終了したか否かを判定する攻撃終了判定工程をさらに含み、

前記経路情報通知工程は、前記攻撃終了判定工程によって前記攻撃パケットの送信が終了したものと判定された場合に、当該攻撃パケットを自己に経由させないための経路情報を前記中継装置に通知することを特徴とする請求項6に記載の防御方法。

[10] ネットワーク上のサーバまたはドメインに対する攻撃情報に基づいて、当該サーバまたはドメイン宛の攻撃パケットを中継する中継装置に対して経路情報を送信して当該攻撃パケットの通過を制御する防御方法を防御装置としてのコンピュータに実行させる防御プログラムであって、

前記攻撃情報に基づいて、自己に隣接する複数の中継装置のなかから前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択する中継装置選択手順と、

前記中継装置選択手順によって中継装置に対して、前記攻撃パケットを自己に経由させるための経路情報を通知する経路情報通知手順と、

前記経路情報通知手順によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットの通過を制御するパケット制御手順と、

をコンピュータに実行させることを特徴とする防御プログラム。

[11] 前記中継装置選択手順は、自己に隣接する複数の中継装置のなかから前記攻撃パケットによる攻撃を受けているサーバまたはドメインに対して次の中継先となる中継

装置を除いて、前記経路情報の通知先となる中継装置を選択することを特徴とする請求項10に記載の防御プログラム。

[12] 自己と隣接関係をもつ他の防御装置に対して前記攻撃情報を送信する攻撃情報送信手順をさらにコンピュータに実行させ、

前記中継装置選択手順は、前記他の防御装置から前記攻撃情報を受信した場合にも、当該攻撃情報に基づいて前記攻撃パケットを自己に経由させるための経路情報の通知先となる少なくとも一つの中継装置を選択することを特徴とする請求項10または11に記載の防御プログラム。

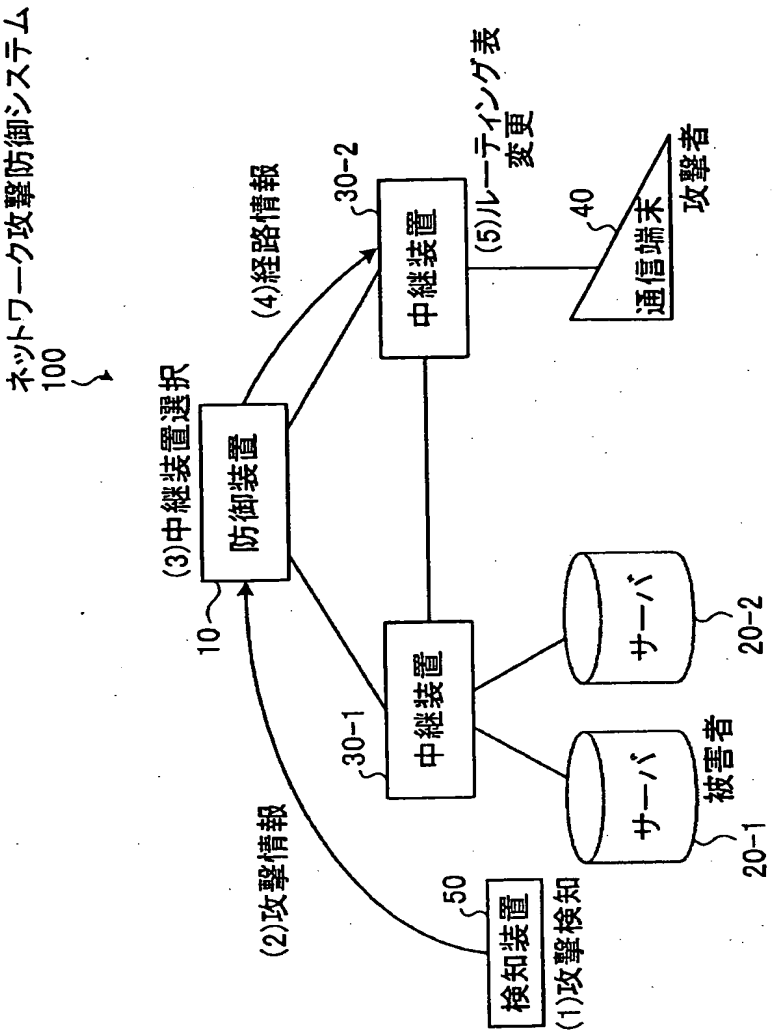
[13] 前記経路情報通知手順によって経路情報が通知された中継装置から自己に経由されてきた前記攻撃パケットを監視して、当該中継装置から自己に経由される攻撃パケットの送信が終了したか否かを判定する攻撃終了判定手順をさらにコンピュータに実行させ、

前記経路情報通知手順は、前記攻撃終了判定手順によって前記攻撃パケットの送信が終了したものと判定された場合に、当該攻撃パケットを自己に経由させないための経路情報を前記中継装置に通知することを特徴とする請求項10に記載の防御プログラム。

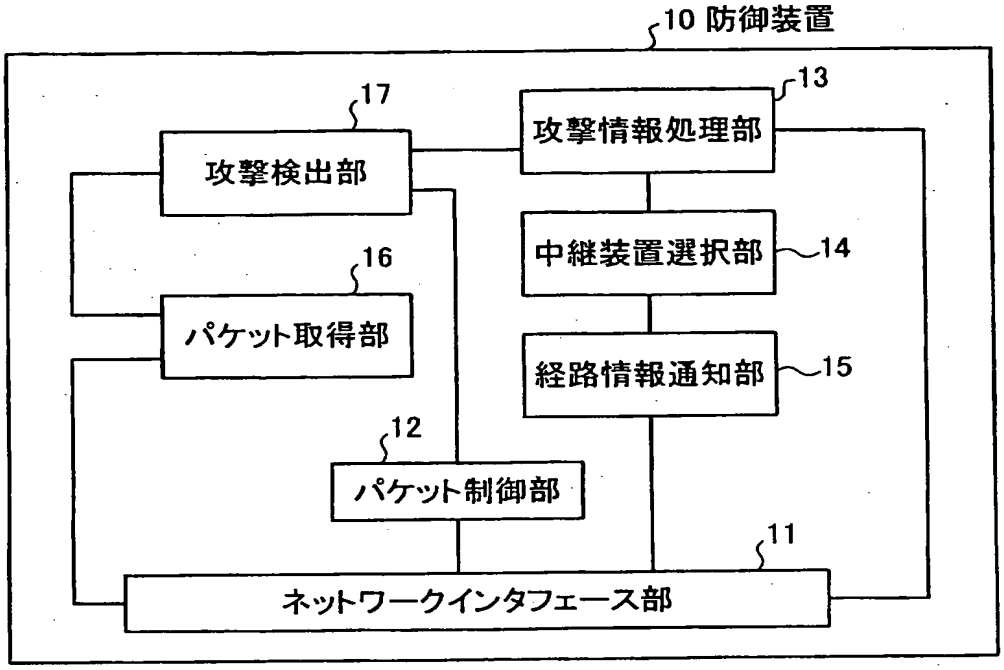
要 約 書

防御装置10は、検知装置50から攻撃情報を受信すると、攻撃情報から攻撃を受けているサーバ20－1を特定した場合には、特定したサーバ20－1に対して次の中継先となる中継装置30－1をルーティング表から求め、防御装置10と隣接する中継装置30－1および中継装置30－2のなかから、この中継装置30－1を除いた中継装置30－2を通知先として選択する。そして、防御装置10は、選択した中継装置30－2に対して、攻撃パケットを自己に経由させるための経路情報を通知し、かかる経路情報に基づいてルーティング表を変更した中継装置30－2から自己に経由されてきた攻撃パケットの通過を制御する。

[図1]


ネットワーク攻撃防御システム
100
(3)中継装置選択
防御装置
10
(4)経路情報
30-2
中継装置
(5)ルーティング表
変更
40
通信端末
攻撃者
中継装置
30-1
サーバ
20-2
サーバ
被害者
20-1
(2)攻撃情報
検知装置
50
(1)攻撃検知

[図2]


10 防御装置
17
攻撃検出部
13
攻撃情報処理部
16
パケット取得部
中継装置選択部
14
経路情報通知部
15
12
パケット制御部
11
ネットワークインタフェース部

[図3]

番号	検出属性(容疑シグネチャ)
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}
2	{Dst=192.168.1.2/32,Protocol=UDP}
3	{Dst=192.168.1.1/24}

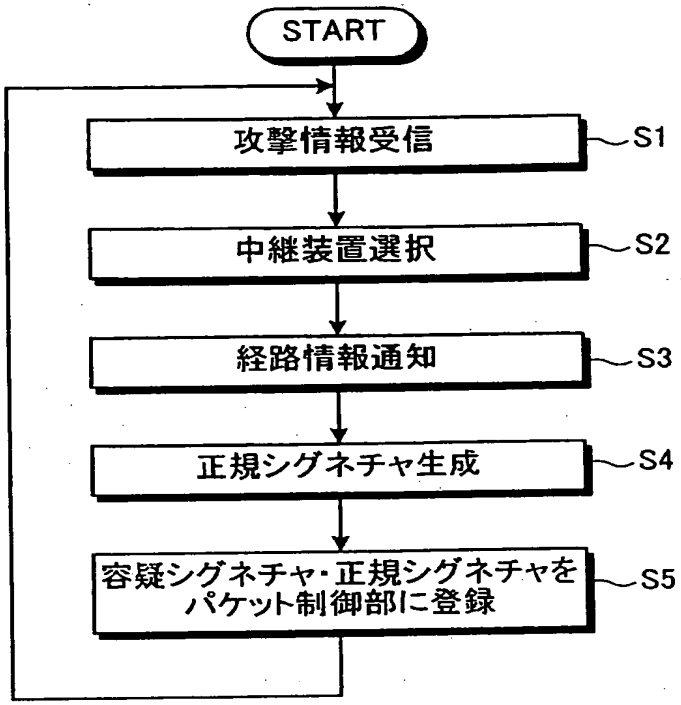
[図4]

番号	検出属性(正規条件)
1	{Src=172.16.10.0/24}
2	{TOS=0x01}

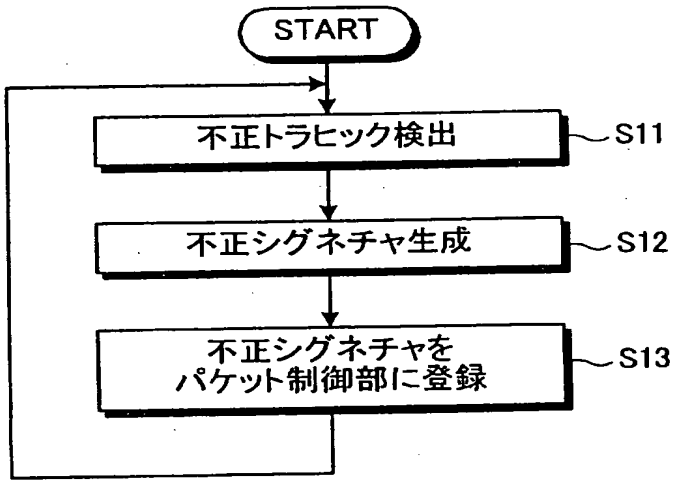
[図5]

番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
1	T3Kbps以上のフラグメントパケットがS3秒以上連続送信されている

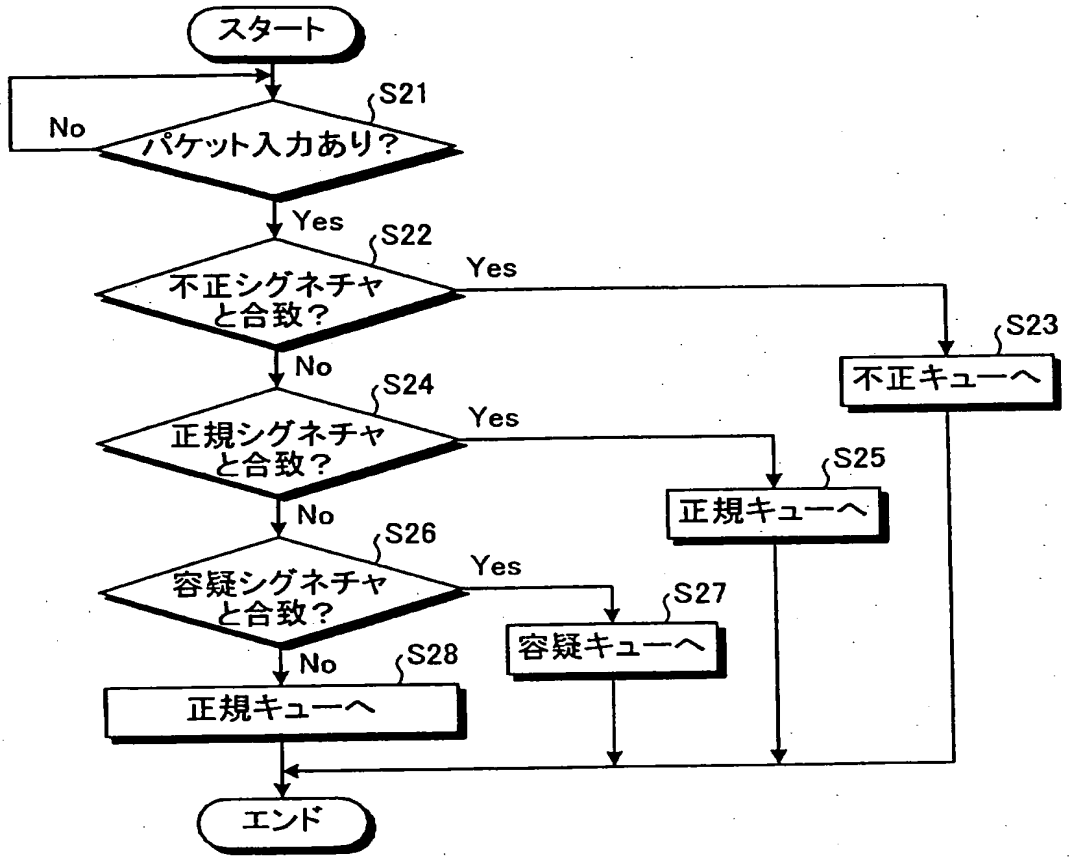
[図6]


START
攻撃情報受信
S1
中継装置選択
S2
経路情報通知
S3
正規シグネチャ生成
S4
容疑シグネチャ・正規シグネチャを
パケット制御部に登録
S5

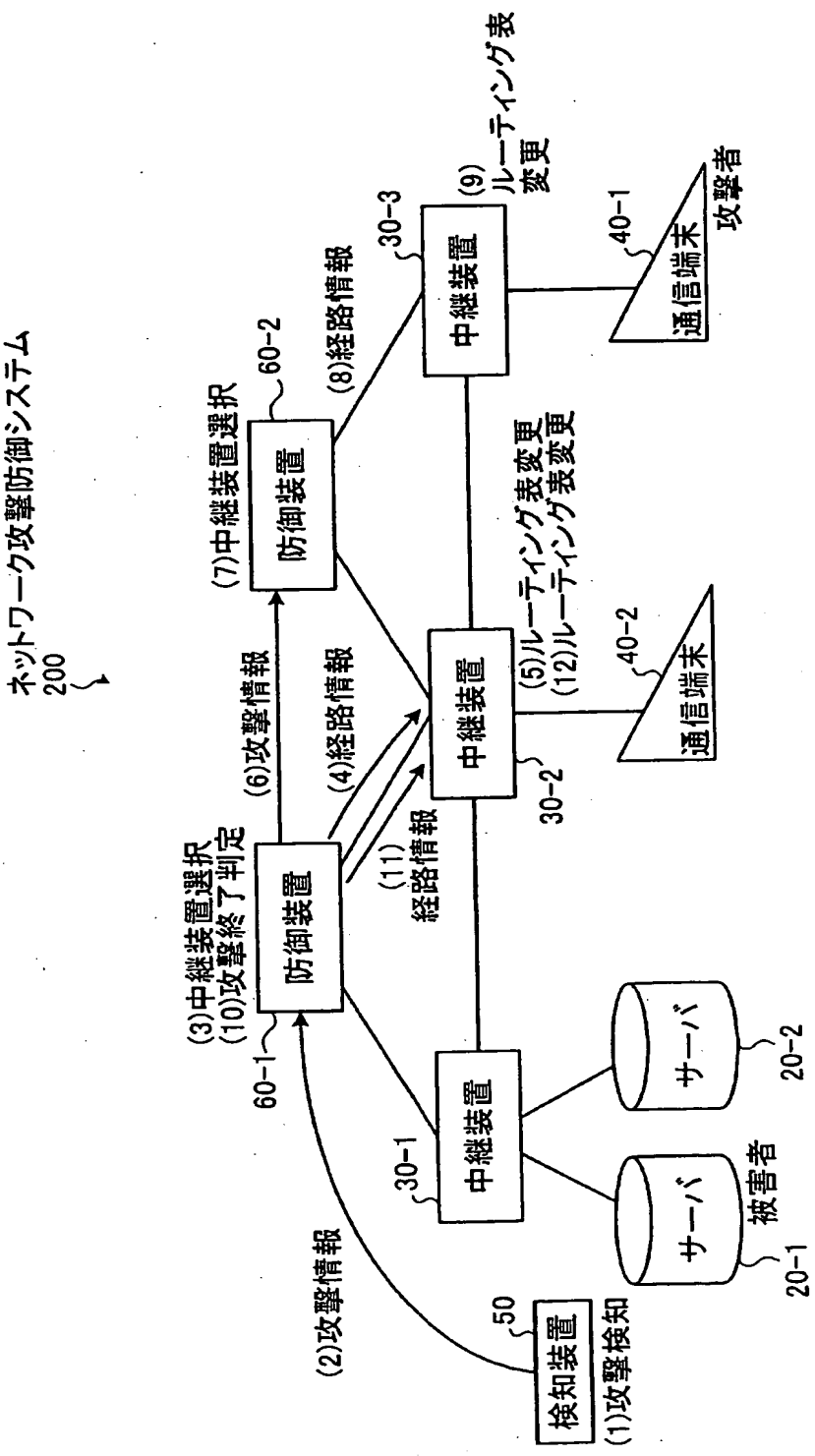
[図7]


START
不正トラヒック検出
S11
不正シグネチャ生成
S12
不正シグネチャを
パケット制御部に登録
S13

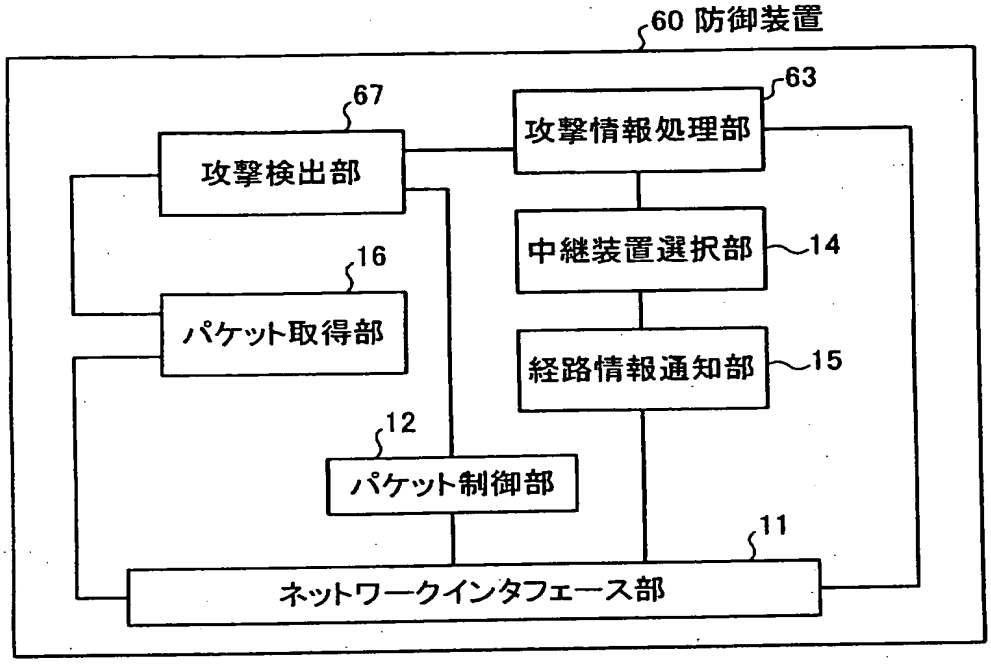
[図8]


スタート
S21
No
パケット入力あり？
Yes
S22
不正シグネチャと合致？
Yes
S23
不正キューへ
No
S24
正規シグネチャと合致？
Yes
S25
正規キューへ
No
S26
容疑シグネチャと合致？
Yes
S27
容疑キューへ
No
S28
正規キューへ
エンド

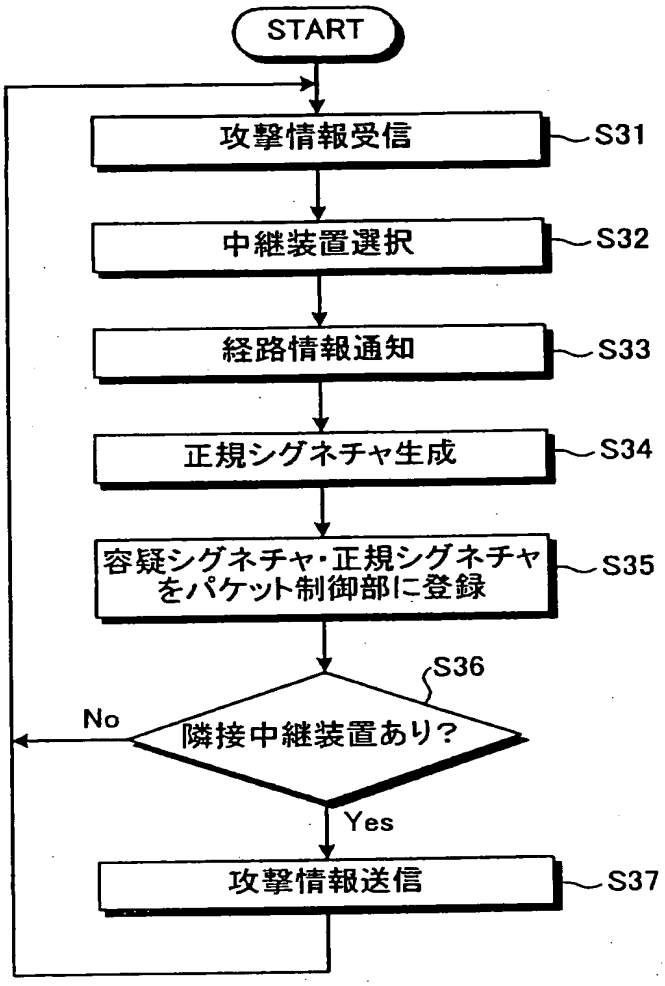
[図9]


ネットワーク攻撃防御システム
200
(1)攻撃検知
(2)攻撃情報
(3)中継装置選択
(10)攻撃終了判定
(4)経路情報
(5)ルーティング表変更
(12)ルーティング表変更
(6)攻撃情報
(7)中継装置選択
(8)経路情報
(9)
ルーティング表
変更
(11)
経路情報
検知装置
50
防御装置
60-1
防御装置
60-2
中継装置
30-1
中継装置
30-2
中継装置
30-3
サーバ
20-1
被害者
サーバ
20-2
通信端末
40-2
通信端末
40-1
攻撃者

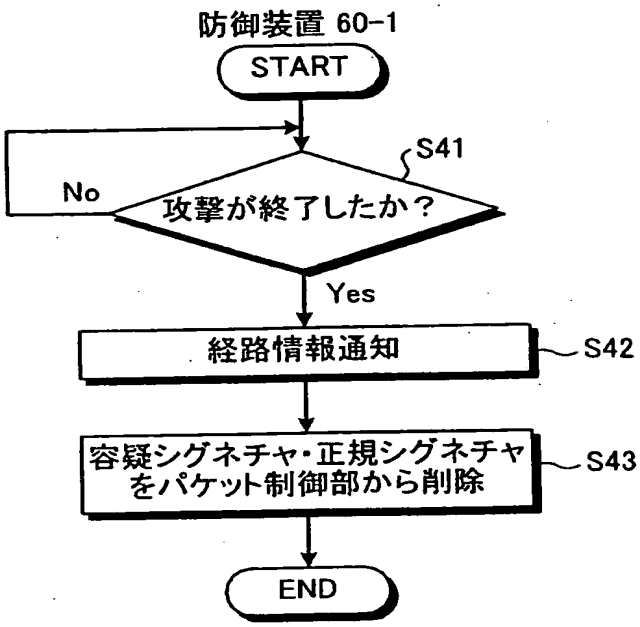
[図10]


60 防御装置
67
攻撃検出部
63
攻撃情報処理部
16
パケット取得部
中継装置選択部
14
経路情報通知部
15
12
パケット制御部
11
ネットワークインタフェース部

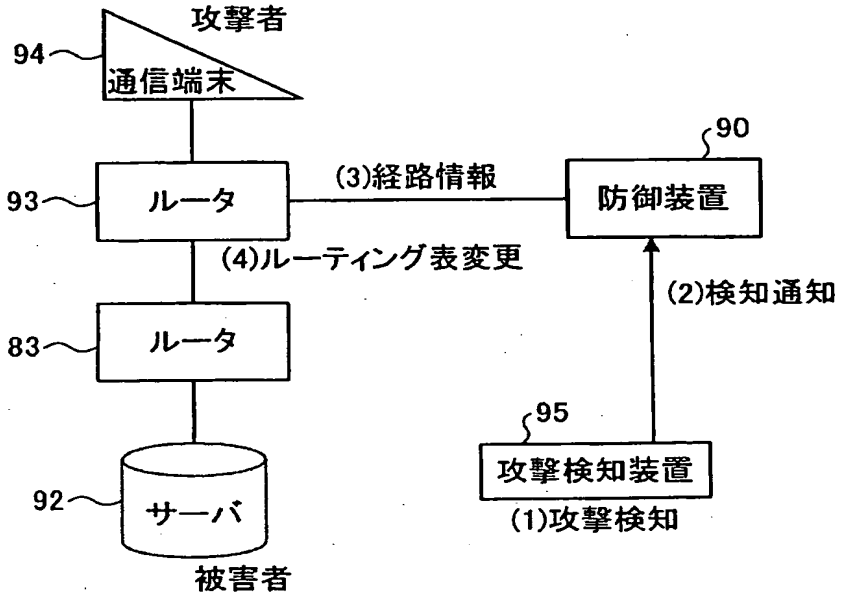
[図11]


START
攻撃情報受信
S31
中継装置選択
S32
経路情報通知
S33
正規シグネチャ生成
S34
容疑シグネチャ・正規シグネチャをパケット制御部に登録
S35
S36
隣接中継装置あり？
No
Yes
攻撃情報送信
S37

[図12]


防御装置 60-1
START
S41
No
攻撃が終了したか？
Yes
経路情報通知
S42
容疑シグネチャ・正規シグネチャ
をパケット制御部から削除
S43
END

[図13]


攻撃者
94
通信端末
90
93
ルータ
(3)経路情報
防御装置
(4)ルーティング表変更
(2)検知通知
83
ルータ
95
攻撃検知装置
92
サーバ
(1)攻撃検知
被害者